Anomaly Detection

Related topics:
- Enabling and Configuring Anomaly Detection
- Troubleshooting Anomalies

AppDynamics Cognition Engine powers Anomaly Detection and Automated Root Cause Analysis, features designed to reduce Mean Time To Resolution for application performance problems. Anomaly Detection automatically tells you whether every Business Transaction in your application is performing normally. Automated Root Cause Analysis helps you quickly determine the root cause for problems revealed by Anomaly Detection.

Anomaly Detection and Automated Root Cause Analysis are available to SaaS customers only.

Anomaly Detection uses Machine Learning to reveal problems automatically

Machine Learning capabilities in Cognition Engine enable Anomaly Detection to estimate Expected Ranges for Business Transaction metrics. When Average Response Time (ART) or Errors Per Minute (EPM) deviate from their Expected Ranges in significant ways, Anomaly Detection alerts you that the Business Transaction has an Anomaly.

An Anomaly is a pattern of abnormal behavior of ART, EPM, or both, for one Business Transaction.

Every Anomaly is a mostly continuous series of Anomaly events. Every Anomaly event has a Severity Level of either Warning or Critical. Anomalies are displayed as timelines which highlight state change events—events where severity is upgraded (changing from Warning to Critical) or downgraded (changing from Critical to Warning).

Anomaly Detection and Health Rules complement each other

While both Anomaly Detection and Health Rules alert you to performance problems in your application, Anomaly Detection provides powerful insights that would be hard or impossible to obtain using Health Rules.

<table>
<thead>
<tr>
<th>Anomaly Detection</th>
<th>Health Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomaly Detection uses Machine Learning to discover the normal ranges of key Business Transaction metrics, and alerts you when these metrics deviate significantly from expected values. This enables Anomaly Detection to identify a wider range of problems than a person could capture in Health Rules.</td>
<td>Health Rules are manually created to apply logical conditions that one or more metrics must satisfy. They are perfect for capturing the clear-cut logic of SLAs, for example.</td>
</tr>
<tr>
<td>Anomaly Detection requires no configuration except when you want to limit Anomaly alerting.</td>
<td>AppDynamics provides a default set of Health Rules and you create additional Health Rules manually as desired, configuring Time Periods, Trends, and schedules.</td>
</tr>
<tr>
<td>An Anomaly is a series of Anomaly events.</td>
<td>A Violation is a series of Health Rule violation events.</td>
</tr>
</tbody>
</table>
Anomalies are associated with Business Transactions.  

Automated Root Cause Analysis saves time and effort

When a Business Transaction in your application has an Anomaly, you will want to know why. AI capabilities in Cognition Engine enable Automated Root Cause Analysis to monitor the health of all entities in your application, and show you Suspected Causes for every Anomaly. You can confirm or negate Suspected Causes with just a brief look, and drill down into deviating metrics and snapshots as desired. In this way, you quickly determine the root cause for application performance problems.